Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1 (currently amended): A method for automatically updating a ciphering key used in a network system, the network system comprising:

a server;

an access point connected to the server for transmitting, via wireless transmission, data received from the server ~~via wireless transmission~~ and also for receiving data transmitted via wireless transmission, the access point using a first ciphering key to encrypt transmission data;

a station for receiving data transmitted from the access point via wireless transmission and transmitting data to the access point via wireless transmission and, the station storing the first ciphering key for encrypting data transmitted to the access point; and

a counting module installed in the server, the access point, or the station, for counting a time;

the method comprising:

~~detonating~~ activating the counting module to start counting the time;

randomly generating a second ciphering key if the time counted by the counting module conforms to a predetermined time;

the access point using the first ciphering key to encrypt the second ciphering key and transmitting the second ciphering key to the station so as to update the first ciphering key stored in the station with the second ciphering key; and

using the second ciphering key to encrypt data transmitted between the access point and the station.

2 (original): The method of claim 1 wherein the station stores an identification data and

the server stores a corresponding registration data, the method further comprising:

before the access point has transmitted the second ciphering key to the station, the access point transmitting a challenge text to the station via wireless transmission;

the station using the first ciphering key stored in the station to encrypt the challenge text into a response text and transmitting the response text to the access point via wireless transmission;

the access point comparing the response text with a standard text;

the station transmitting the identification data of the station to the access point via wireless transmission if the response text matches the standard text;

the access point transmitting the identification data of the station to the server; and

the access point transmitting the second ciphering key to the station if the identification data of the station matches the registration data stored in the server.

3 (original): The method of claim 2 wherein the standard text is generated from encrypting the challenge text with the first ciphering key.

4 (original): The method of claim 1 further comprising requesting a response from a user of the station before updating the first ciphering key of the station with the second ciphering key.

5 (original): The method of claim 1 wherein the station uses the second ciphering key to decrypt the data received from the access point after the first ciphering key of the station is updated with the second ciphering key.

6 (currently amended): The method of claim 2 wherein the network system comprises a plurality of stations, and each station stores the first ciphering key and ~~the~~ corresponding identification data.

7 (original): The method of claim 1 wherein the second ciphering key is randomly generated by a random-code generation program.

8 (original): The method of claim 1 further comprising:

the access point transmitting a confirmation challenge text to the station via wireless transmission after the second ciphering key is transmitted to the station;

the station using the second ciphering key to encrypt the confirmation challenge text into a confirmation response text and transmitting the confirmation response text to the access point via wireless transmission; and

the access point comparing the confirmation response text with a confirmation standard text.

9 (original): The method of claim 1 wherein the counting module is a real time clock (RTC) for counting a real time.